For Consumers

Beware of Scams

Fraudsters will take advantage of customer's:

Fear of uncertainty

Need of quick Corona Virus Relief payments

WE
CAN
HELP

Fraud Tips for Consumers

Important Information

No Financial Institution or organization can guarantee that they can obtain early access to government funding.

Government relief payments to individuals will utilize the individual's most recent income tax information to remit payment.

Do not send payments to obtain early funding or payments from government programs.

Fraud Tips: Who contacts you

US government

- For relief payments, the government should not be contacting consumers directly by text, phone call, or email. The government will be using information from your recent tax return.
- The government will normally contact consumers through the U.S. Postal Service mail.
- The government does not have the consumer's information to text, call or email.

AMERICAN Savings Bank

American Savings Bank – if we contact you via

- Text — We will never ask for account, password/PIN information.
- Call — There should be a person on the line. We do **not** use automated calling.
- Email — Is to notify you to check your secured message box in online banking.

Fraud Tips for Consumers

Prevention Tips – When your are contacted:

- Before responding, ask these questions:
  - Do I know the person/organization who is contacting me?
  - Is this how this person/organization normally contacts me?
  - Are they asking me for my PIN, Online banking log in and password, asking me to send money?

Beware of unsolicited calls!

Prevention Tips – When your are contacted:

- Thoroughly check the email address of the Email Senders
  - **On your phone**: Click on the name of the person/organization sending the email to reveal the sender's email.

- **On you computer:** Using your mouse, hover over the name of the person sending the email to reveal the sender's email.

- Emails can say it is from a company, but when you review it, the sender email is different. Example - email address that normally says Jdoe@123Company.com, but new email is from Jdoe@Company.com.

Fraud Tips for Business Customers

Prevention Tips – When your are contacted:

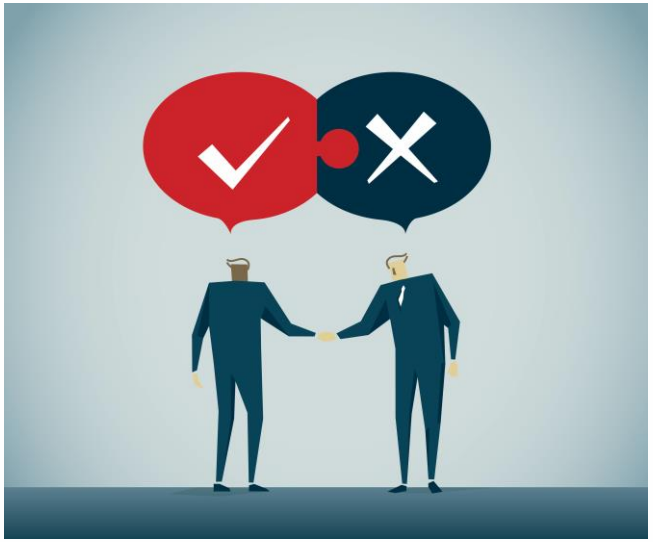
- Validate the Contact – Look up the contact's information online or through the phone book. Call that number and ask for the person.

- If at any time you are asked for private information (your account number, online banking log in an password, or card number and PIN), STOP the conversation.

Fraud Tips for Consumers

Prevention Tips – When your are contacted:

- Job or loan offers or Loan offers you did not apply for.
  - Offers sent to you, that you did not apply for are normally a scam.
  - If you did apply for a loan or job online. Do not provide your online banking log in and password to obtain funds.



Fraud Tips for Consumers

Prevention Tips – When your are contacted:

- Contact is asking for some type of payment
  - Send funds to get to get funds – Beware! This is a scam
  - Send reimbursement because your account was credited too much. Could be a scam. Check your accounts to ensure funds were not transferred from another one of your accounts on your online banking.
  - Help a person you met online by using your account to deposit funds and send out.

Fraud Tips for Consumers

Prevention Tips – When your are contacted:

- Beware of emails with attachments.
  - Emails from senders you do not know.
  - Attachments with .exe extensions.
  - Suspicious emails can have virus or malware.

Fraud Tips for Consumers

Prevention Tips for Account Fraud

Review your Account Activity/Statements regularly

- Use online banking/mobile banking to review account activity for unauthorized transactions. Review daily if possible.
- Carefully review electronic transactions (ACH, debit card transactions) to your account.
- Notify the Bank immediately of any unauthorized transactions.

Additional Information on Consumer Fraud can be found at the Federal Trade Commission website: https://www.consumer.ftc.gov

Fraud Tips for Consumers

What should I do if I am a victim of Fraud?

- Contact your bank immediately for assistance
  - Provide as much information as you can about what happened.
  - If and how you were contacted and by who.
  - Indicate what information you may have given out
  - Notify of any unauthorized transactions.
- Check your Credit Report.

- As applicable, report any identity theft to the Federal Trade Commission. Website: https://www.ftccomplaintassistant.gov

- As applicable, file a police report.